

المؤتمر الثالث
لرؤساء المحاكم العليا بالدول العربية

في الفترة من ٢٣-٢٥ سبتمبر ٢٠١٢م - بالخرطوم

دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول



الشيخ / أحمد بن عبد الرحمن البعادي
عضو المحكمة العليا



إعداد:
إدارة الدراسات والبحوث
1433هـ

بسم الله الرحمن الرحيم

تمهيد:

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين، أمَّا بعد:

إنَّ من أهم إنجازات العلم الحديث في هذا العصر وأعظمها جدوى للإنسان ظهور الحاسب الآلي والإنترنت، وما حقّقته تكنولوجيا المعلومات والاتصالات من فوائد عديدة في مجال الرقيّ والتقدُّم الإنساني في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية والعديد من المجالات الأخرى.

لكن رافق هذه الانجازات بروز خبراء جدد لم تعهدهم الإنسانية من قبل، يتمتعون بالخبرة والحرفية في تطويع هذه التقنية للقيام بأعمال إجرامية أفرزت إلى جانب الجريمة التقليدية الجرائم المعاصرة، بل حوَّلت هذه الجريمة من صفتها العاديّة، وأبعادها المحدودة إلى أبعاد جديدة تعتمد التقنية في تنفيذ الفعل المجرّم، وبأساليب مبتكرة، وطرق جديدة لم تكن معروفة من قبل.[1]

(1) وهنا تبرز حقيقة واضحة ثابتة هي: أنَّ وسائل الاتصال لم تخترع الجريمة؛ بل كانت كغيرها ضحيَّة لها في معظم الأحوال، وعرضة لسوء الاستغلال مِنْ قِبَل المنحرفين عبر التاريخ الإنساني.

=

وساعد هؤلاء المجرمين ما يشهده العصر من تطور الوسائل المعلوماتية الحديثة، في زيادة سرعة نشر جرائمهم حتى أصبحت تهدد النظام المعلوماتي، بل أصبح في إمكانهم التسبُّب في خلق شلل كامل للأنظمة المدنيّة والعسكريّة، الأرضيّة والفضائيّة، وتعطيل المعدّات الإلكترونيّة، واختراق النُّظم المصرفيّة، وإرباك حركة الطيران وشل محطات الطاقة وغيرها بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الكمبيوتر من على مسافات تتعدّى عشرات الآلاف من الأميال، وذلك دون أن يترك المجرم المعلوماتي أو الإلكتروني أثرًا ملموسًا لملاحقته ومعرفة مَصدرها. والجاني يستطيع بواسطة هذه التقنيات العالية أن يصل إلى أي مكان يرغب فيه، عبر الإبحار في الشبكة المعلوماتية ويتصل ويتفاعل مع من شاء في أي مكان ,فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة. ولاشك أنَّه من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم المعلوماتية، فالمواجهة التشريعية ضرورية للتعامل من خلال نظم قانونية غير تقليدية لهذا الإجرام غير التقليدي، هذه المواجهة تتعامل بشكل عصري متقدم مع جرائم الكمبيوتر المختلفة، التي يأتي في مقدمتها الدخول غير المشروع على شبكات الحاسب ونظم المعلومات، والتحايل على نظم المعالجة الآلية للبيانات ونشر الفيروسات وإتلاف البرامج وتزوير المستندات، ومهاجمة المراكز المالية والبنوك وتعدتها إلى الحروب الإلكترونية، والإرهاب الإلكتروني، ونشر الشائعات والنيل من هيبة الدول، إضافة إلى نشر الرذيلة والإباحية وغيرها من الجرائم الإلكترونية، وقد لفتت بالفعل هذه الأعمال الإجراميّة أنظار الدول والهيئات الدولية التي أدركت خطورتها وسهولة ارتكابها وتأثيرها المباشر؛ لتجعل مكافحتها من أولى أولويات المجتمع الدولي والحكومات، ما حتّم أهمية الحماية القانونية لمواجهة هذه الأفعال الإجرامية.[2]

فجاءت هذه الورقة المعنون لها بـ: «**دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول**»، ضمن فعاليات المؤتمر الثالث لرؤساء المحاكم العليا (النقض، التمييز،

=

انظر: د. فايز بن عبدالله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد20، العدد 39، (ص133 و144).

(2) اللواء د. حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية (تصور مقترح) (ص5 – 6) المجلة العربية للدراسات الأمنية والتدريب المجلد 27 العدد 53. بتصرف.

وانظر: مهندس. فاروق سيِّد حُسَيْن، الانترنت – الشبكه العالميه للمعلومات.

التعقيب) في الدول العربية المنعقد في جمهورية السودان الشقيقة خلال الفترة 23-25/9م الموافق 7-1433/11/9هـ.

وقد اشتملت على أربعة مباحث:

المبحث الأول: مقدِّمات تعريفيَّة.

المبحث الثاني: أدلة إثبات الجرائم الإلكترونية في الشريعة الإسلامية.

المبحث الثالث: أدلة إثبات الجرائم الإلكترونية في التشريعات العربية.

المبحث الرابع: صعوبات إثبات الجريمة الإلكترونية.

التوصيات والمقترحات.

***

المبحث الأول
مقدِّمات تعريفيَّة

- تعريف الجريمة الإلكترونية:

تعدَّدت ألفاظ ومفردات وصِيَغ ومصطلحات التعريف بالجريمة الإلكترونية تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد، فأُطْلِقَ على الجريمة الإلكترونية هذا المسمَّى (crime-e)، وجرائم الكمبيوتر والإنترنت، وجرائم الحاسب الآلي (Computer Crimes)، وجرائم التقنية العالية (High-Tick)، والجرائم المعلوماتيّة (Information Crimes)، والجرائم الرقمية (Digital Crimes)، والسيبر كرايم (Cyber Crime)، وجريمة أصحاب الياقات البيضاء (White Collar)، والجرائم الناعمة[3] (Soft Crimes)، والجرائم النظيفة[4] (Clean Crimes).

---

(3) فهي جرائم لا تتصف بالعنف أو القوة عند ارتكابها، ولكنها تتسم بلمسات بسيطة لا تستغرق ثوان معدودة. انظر: د. ناول عبدالهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427.

(4) وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأيِّ عنف أو دماء، وإنما مجرد أرقام وبيانات. انظر: محمد علي العريان، الجرائم المعلوماتية، (ص35 – 36)، نقلا عن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، 19 – 20 نيسان/ يونيو، 2007، المملكة المغربية (ص52).

وقديمًا عرَّف العلامة الماورديُّ من علماء المسلمين من أئمَّة الشافعيَّة (ت: 450هـ) **الجرائم** بأنها: (**محظورات شرعية، زجر الله تعالى عنها بحدّ أو تعزير**).[5] وحتى اليوم ما زال هذا التوصيف صالحًا ليشمل جرائم الإنترنت؛ لأنها في أفعال تستهدف محظورات، ولكن وِفْق أساليب جديدة.[6]

وقد تحدَّث الفقه القانوني المعاصر طويلًا حول التعريف العلمي القانوني للجريمة الإلكترونية، وتعدَّدت المدارس والاتجاهات في ذلك، ومن أحسن وأجمع وأشمل هذه التعاريف، تعريف **منظمة التعاون الاقتصادي والتنمية** (OCDE)؛ إذْ عَرَّفت **الجريمة المعلوماتية** في اجتماع باريس عام (1983م) بأنها: (**كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآليّة للبيانات أو نقلها**).

وعَرَّف **نظام مكافحة جرائم المعلوماتية السعودي**، الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 1428/3/8هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 1428/3/7هـ **الجريمة المعلوماتية بأنها**: (**أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أوالشبكة المعلوماتية بالمخالفة لأحكام هذا النظام**).[7]

***

- صُوَر الجريمة المعلوماتية وهي كثيرة منها:

1- **الدخول غير المشروع في نُظُم وقواعد معالجة البيانات**، سواء أحدثَ هذا الدخول تلاعبًا أو لا.

(5) الأحكام السلطانية (ص322). وانظر: عبد القادر عودة، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي (66/1).

(6) انظر: د. فايز بن عبدالله الشهري، دراسة الظاهرة الإجرامية على شبكة الإنترنت، مصدر سابق (ص153).
وانظر: د. عارف خليل أبو عيد، جرائم الإنترنت - دراسة مقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5 العدد 3 (ص82).

(7) انظر: الأستاذة سميرة معاشي، مجلة المنتدى القانوني، ماهية الجريمة المعلوماتية، (ص275 - وما بعدها)، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، (1432 هـ 2011م)، جامعة نايف العربية للعلوم الأمنية (ص63 - وما بعدها).

2- **الاعتداء على المواقع الإلكترونية** سواء كان ذلك بمسح أو تعديل بيانات أو التلاعب فيها، أو إعاقة تشغيل النظام.

3- **انتهاك السريَّة والخصوصيَّة للبيانات الشخصيَّة**، والإضرار بصاحبها، والإطّلاع على المراسلات الإلكترونية، والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية.

4- **الاعتداء على الأموال الإلكترونية** – وهي الأموال المتداولة إلكترونيًّا – سواء أكان ذلك في إطار التجارة الإلكترونية أو غيرها، مثل عمليات سحب وإيداع الأموال التي تقوم بواسطة أجهزة الصراف الآلي أو الهاتف المصرفي أو الخدمات المصرفية بواسطة الإنترنت للبنوك؛ إذْ يمكن أنْ تتعرّض هذه الأموال للسرقة والنصب وخيانة الأمانة، وذلك بواسطة بطاقات ائتمان مزورَّة أو انتهت صلاحيتها أو مسروقة، أو إختراق المواقع الإلكترونية للبنوك،أو اختراق أجهزة الحاسب الآلي للبنوك أو عملاء البنوك...الخ .

5- **التعدي على أموال غيره بالوسائل الإلكترونية** مثل: الدخول لمواقع البنوك والدخول لحسابات العملاء وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو تحويلها من حساب لآخر.

6- **تزوير أو تقليد التوقيع الإلكتروني** الذي هو عبارة عن رموز تميِّز صاحب هذا التوقيع، وهو بهذا المعنى يعد وسيلة تعتمد في المعاملات الإلكترونية ويقوم مقام التوقيع الكتابي.(8)

***

- خطورة الجرائم الإلكترونية:

---

(8) انظر: السيد عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، 20 - 19 نيسان/ يونيو، 2007، المملكة المغربية، (ص69).

وللمزيد، ينظر: المهندس حسن طاهر داود، جرائم نُظُم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض 1420 هـ 2000م , جرائم الإحتيال والإجرام المنظَّم، المجلة العربية للدراسات الأمنية والتدريب المجلد 24 العدد 48 (ص293 – وما بعدها), أ.د. محمد حسن الطائي، أمن المعلومات – مجالات الاختراق وآلية التعزيز، المجلة العربية للدراسات الأمنية والتدريب المجلد 20 العدد 40, د. ناول عبدالهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427, د. عارف خليل أبو عيد، جرائم الإنترنت – دراسة مقارنة، مصدر سابق، (ص84).

إنَّ ظاهرة الجرائم الإلكترونية ظاهرة إجراميّة مُستجدَّة نِسبيًّا تقرع في جنباتها أجراس الخطر لتنبِّه مجتمعات العصر الرّاهن لحجم المخاطر، وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة: **بيانات، ومعلومات، وبرامج بكافّة أنواعها**؛ فهي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، تُوَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الكمبيوتر المخزَّنة، والمعلومات المنقولة، عبر نُظُم وشبكات المعلومات، وفي مقدمتها الإنترنت.(9)

وقد بلغت **عدد الشكاوى** التي تلقَّاها مركز شكاوى احتيال الإنترنت الأمريكي (IFFC) منذ بدأ اعماله في أيار (2000م) وحتى شهر تشرين ثاني من العام نفسه (أي خلال ستة أشهر فقط) (6087) شكوى، من ضمنها (5273) حالة تتعلق باختراق الكمبيوتر عبر الإنترنت، وقد بلغت الخسائر المتصلة بهذه الشكاوى ما يقارب (4.6)مليون دولار.

وأعلن مركز بلاغات جرائم الإنترنت Internet crime complain center (IC3) في تقريره السنوي لعام (2007م) أن مقدار ما تم خسارته في تكاليف الاستقبال (الاستقبال فقط) للبلاغات الناتجة من سوء استخدام الانترنت هو 198.4مليون دولار وذلك بزيادة قدرها (15.3) مليون دولار عن السنة التي قبلها.

ثم إنَّ **"الفاتورة" الإجمالية لجرائم أمن المعلومات** عالميًّا وعربيًّا في (**2011م**) وحدها تُقدَّر بحوالي (388) مليار دولار أميركي، أما التكلفة النقدية المباشرة لهذه الجرائم المتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي (114) مليار دولار، ومعنى ذلك أنَّ القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين التى تقدر بحوالى (288) مليار دولار، وتزيد عن قيمة السوق العالمية للمخدرات عموما التى تصل إلى (411) مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة (اليونيسيف) بحوالى 100 ضعف، حيث تصل ميزانيتها إلى (3.65) مليار دولار، كما تعادل هذه

(9) انظر: د. يونس عرب، جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10 ، 2002/2/12.

الخسائر ما تم إنفاقه خلال 90 عامًا على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38 عاما.

وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثَّر بها (589) مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من إجمالي سكان العالم. وقد توزَّعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة.

ولقد شهد العام الماضي (2011م) كثير من الحوادث والمواجهات في عالم أمن المعلومات، حملت كثير من الدلائل على أنَّ الأمر تخطَّى كل الحدود المعتادة، وصار جولات صراع مكشوفة بين الدول بعضها مع بعض، حتى أنَّ **جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي**؛ فعلى سبيل المثال إذا ما أخذنا بعين الاعتبار ما تم اكتشافه بخصوص فيروس دوكو (Duq)، فسنجد أن نتائج الدراسات الخاصة بحماية البنية التحتية الحساسة مقلقة؛ إذ الغرض الذي صمّم من أجله فيروس دوكو هو جمع المعلومات الاستخباراتية ومعلومات عن الأصول (Assets) من منظمات معيّنة مثل الشركات المصنّعة للمكونات التي توجد عادة في بيئة التحكم الصناعي، كما أن من يقفون وراء هجوم دوكو كانوا يبحثون عن معلومات مثل وثائق التصميم التي يمكنها أن تساعدهم في المستقبل لشن هجوم على منشآت التحكم الصناعي. ويمثِّل "دوكو" الجيل الأحدث من ستكسنت (Stuxnet) التي ذكرت تقارير عديدة أن الأميركيين استخدموه في إحداث فوضى داخل البرنامج النووي الإيراني, وفي هذه المرحلة فإن من غير المبرّر الاعتقاد بأن من يقف وراء هجوم "دوكو" لم يتمكن من الحصول على المعلومات الاستخباراتية التي يبحث عنها، وإضافة إلى ذلك فمن المحتمل أن هجمات أخرى لجمع المعلومات قد بدأت بالفعل ولم يتم اكتشافها بعد. وخلال عام (2011م) عرف العالم جماعات متخصصة من القراصنة الإلكترونيين، مثل (Anonymous) و(LulzSec) وغيرهما؛ حيث استهدفت تلك الجماعات الشركات والأفراد لتحقيق مآرب سياسية مختلفة. ويرجّح خبراء شركة تريند مايكرو -إحدى الشركات الدولية المتخصصة في أمن المعلومات-

أن تزداد أنشطة مثل هذه الجماعات خلال عام 2012، بل تزداد قدرتها على اختراق شبكات الشركات والإفلات من محاولات رصدها ومقاضاتها.(10)

وأمَّا الخطورة الأخلاقية؛ فإنَّ جلّ جرائم الإنترنت تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية، إمّا بسبب المنافسة، أو بداعي الانتقام، ونحو ذلك. وأيضًا على شبكة الإنترنت تنشط تجارة الدعارة والصور الخليعة التي تُعدّ أكبر صناعة نشطة على شبكة الإنترنت بحجم عائدات كبير يُقَدَّر بنسبة 58% من مجمل عائدات الخدمات المدفوعة على الشبكة لعام (2003م).

وعبر آلاف المواقع تُنشَر صور فاحشة، وتُقَدَّم خدمات جنسيّة مدفوعة، وتُستغل صور الأطفال والمشاهير في أوضاع شائنة، دون أن تنال كثيرًا من هذه الأنشطة يد القوانين المحليّة أو الدولية.(11)

وأمَّا الخطورة الأمنية والمجتمعيَّة فقد لا يُدرك كثيرون أنّ الجماعات المتطرّفة كانت من أوائل الجماعات الفكريّة التي دخلت العالم الإلكتروني حتى قبل أنْ تظهر شبكة الإنترنت بسنوات.

وممّا تشير إليه المصادر الغربيّة أنَّ «توم ميتزقر» (Tom Metzger) أحد أشهر المتطرّفين الأمريكيّين العنصريّين (اليمين المتطرّف) ومؤسّس مجموعة المقاومة «الإريانية البيضاء» (White Aryan Resistance) كان مِن أوائل مَن أسّس مجموعة بريد إلكترونيّة ليتواصل مع أتباعه ويبثّ أفكاره سنة (1985م).

ومما غاب عن بعض الباحثين أنَّ المجموعات البريدية الإلكترونية كانت الأكثر توظيفًا مِن قِبَل الجماعات العِرقيّة المتطرّفة قبل ظهور الإنترنت التجاري، وربما ظلت على هذا النمط حتى ما بعد منتصف التسعينيات. وقد عُرفت جماعات كثيرة عبر شبكات المعلومات ما قبل الإنترنت مثل مجموعة المتطرف الأمريكي «دان جانوون» (Dan Gannon) الذي يعد بحسب المصادر الغربية أول

---

(10) المعلومات الواردة بتقدير حجم جرائم المعلومات عالميا وعربيا، اعتمادًا على تقرير The Norton Cybercrime Report 2011 الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام 2011، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم". نقلا عن مركز الجزيرة للدراسات.

(11) د. فايز بن عبدالله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، مصدر سابق (ص154 – وما بعدها).

من أنشأ موقعًا متطرِّفًا يَبثّ من خلاله أفكاره العُنصريّة عن نقاء العرق الأبيض في شهر ديسمبر (1991م) مع ولادة الإنترنت في الولايات المتحدة.

وتلَى ذلك عدة مجموعات اشتهر منها بعد ذلك مجموعة «جبهة العاصفة» (Stormfront) الأمريكية المسيحية المتطرفة بقيادة «دون بالك» (Don Black) التي أنشأت أول موقع متكامل عن التطرُّف وثقافة الكراهية في مارس سنة (1995م).

وقد تتالى ظهور مواقع تابعة لجماعات متطرِّفة من الولايات المتحدة وأوروبا وبشكل خاص بريطانيا وأستراليا، ثم بقية دول العالم.

وفي كل هذه المراحل كان الإنترنت في عمق دائرة ترويج ثقافة التطرُّف والعنف، معبِّرة عن أفكار المهمَّشين والمتطرِّفين الصاحبين من كل ملة وجنس.

وفي العالم الإسلامي أسهمت شبكة الإنترنت بشكلٍ واضحٍ في بَسط نفوذ التطرُّف الفكري لمختلف التيارات من خلال المواقع والمنتديات التي تديرها الجماعات والرموز المتطرفة التي تقدم منتجاتها الفكرية وفق خطاب جاذب، مستغلّين في ذلك الواقع المر في كثير من مجتمعات العالَمَيْن العربي والإسلامي.

ومع أنَّ التطرُّف لا دين له ولا جنس، إلا أنّ ما أصاب المسلمين من شرر التطرُّف في العقود الماضية خاصَّة حين قاد إلى العنف يتجاوز ما حصل لبقية شعوب الأرض. في المجتمع العربي كانت تأثيرات القادم الجديد (الانترنت) قد بدأت تتشكّل حين وفّرت الشبكة فضاءً حُرًّا لنشر كل «ممنوع» منذ بداياتها الأولى لتصبح مع مطلع الألفية الثالثة الوسيلة الأبرز في ترويج التطرف والعنف والكراهية، ما جعل من المتطرفين سادة المشهد الإلكتروني خاصة بعد أحداث الحادي عشر من سبتمبر.[12]

---

(12) استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية، الرياض، 1433 هـ 2012م.

وانظر: أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، 20 - 19 نيسان/ يونيو، 2007، المملكة المغربية، محمود شاكر سعيد؛ تقرير عن: ندوة التخطيط الأمني لمواجهة عصر العولمة، المجلة العربية للدراسات الأمنية والتدريب المجلد 20 العدد 40 (ص295 – وما بعدها)؛ التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية – دراسة مسحية تحليلية، مركز المعلومات في جامعة نايف العربية للعلوم الأمنية؛ لمياء إبراهيم المنيع، تأثير =

***

- مكاف□ة الجرائم الإلكترونية "من الزاوية النظاميّة والقانونية":

تزايدت خطط مكافحة الجرائم الإلكترونية، وانصبَّت الجهود على دراستها المتعمِّقة، وخلق آليّات قانونيّة للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، خاصة المنظمات والهيئات الإقليميّة الأوروبية. وإدراكًا لقصور القوانين الجنائيّة بما تتضمّنه من نصوص التجريم التقليديّة عن أن تحيط بالجرائم الإلكترونية ، كان لا بد للعديد من الدول من وضع قوانين وتشريعات خاصّة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم. وأظهر تحليل الجهود الدولية، واتجاهات القانون المقارن بشأن جرائم الكمبيوتر والإنترنت أنّ مواجهة هذه الجرائم تم في ثلاثة قطاعات مستقلة:

1- حماية استخدام الكمبيوتر، أو ما يُعرَف أحيانًا بجرائم الكمبيوتر ذات المحتوى الاقتصادي.

2- حماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية).

3- حماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية).

وفيما يأتي نذكر جملة من القوانين الدولية والعربية التي ساهمت في مكاف□ة الجريمة الإلكترونية:

1-قانون البيانات السويدي عام (1973م):

تعتبر السويد أول دولة تسن تشريعات ضد جرائم الإنترنت أو جرائم المعلوماتية، لا سيَّما التزوير المعلوماتي؛ حيث صدر قانون البيانات السويدي عام (1973) الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها.

2-قانون مكاف□ة جرائم ال□اسب الآلي والانترنت الدنماركي (1985م):

وفي عام 1985 سنَّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت التي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الألي كالتزوير المعلوماتي.

3-قانون مكاف□ة التزوير والتزييف البري□اني (1986م):

=

الجرائم الإلكترونية على النواحي الاقتصادية، مركز التميُّز لأمن المعلومات؛ د. عارف خليل أبوعيد، جرائم الإنترنت – دراسة مقارنة، مصدر سابق، (ص84 – وما بعدها)؛ شبكه الانترنت، ما لها، وما عليها، المركز العربي للبحوث التربوية لدول الخليج، الدورة السابعة للموسم الثقافي التربوي للمركز، 1420هـ 2000م.

أصدرت بريطانيا قانون مكافحة التزوير والتزييف عام (1986م)، الذي شمل في تعاريفه الخاصة تعريف أداة التزوير، وهي: (وسائط التخزين الحاسوبية المتنوّعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى).

4-قانون مكافحة التزوير المعلوماتي الألماني (1986م):

سَنَّ المشرِّع الألماني قانون مكافحة التزوير المعلوماتي سنة (1986م).

5-القانون الفرنسي الخاص بالتزوير المعلوماتي (1988م):

أصدرت فرنسا في عام (1988م) القانون رقم 19 الخاص بالتصدِّي للتزوير المعلوماتي.

6-اتفاقية الإجرام السيبيري (الإجرام عبر الانترنت) (2001م):

صدرت هذه الاتفاقية عن المجلس الأروبي، ووُقِّعَت في العاصمة المجرية بودابست في 23 نوفمبر (2001م)، وقّعت عليها 30 دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في 22 سبتمبر (2006)م، ودخلت حيز النفاذ في الأول من يناير (2007م). واشتملت على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

7-قانون مكافحة الجرائم الإلكترونية (مواده مستحدثة ضمن أ□كام قانون الجزاء العماني)، بسلطنة عُمَان (2001م):

أصدرت سلطنة عمان جملة من التشريعات لمكافحة الجريمة المعلوماتية تحت مسمى: قانون سلطنة عمان لمكافحة جرائم الحاسب الآلي ، فقد صدر المرسوم السلطاني رقم (72) لسنة (2001 م) بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر)، وذلك بإضافة فصل في الباب السابع من قانون الجزاء العماني تحت عنوان (جرائم الحاسب الآلي). وكذلك أضيفت مواد إلى قانون الاتصالات العماني تحرم تبادل رسائل تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد ، وأسست السلطنة قانوناً ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة.

8-المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي:

أدخل المشرِّع المغربي الفصول التي تعاقب على الأفعال التي تشكل جرائم عنوان (المس بنظام المعالجة الآلية للمعطيات) وذلك بموجب القانون رقم 07.003 الصادر بتاريخ 16 رمضان 1424 الموافق 11 نوفمير 2003.

9-قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها (2003م):

قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم (495 - د 19 – 10/8/ 2003) ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (417 - د 2004/21).

10-قانون مكافحة الجرائم المعلوماتية الإماراتي (2006م):

تعتبر دولة الإمارات العربية أول دولة عربية تسن قانونًا مستقلًّا لمكافحة الجرائم المعلوماتية رقم 2 لسنة (2006م).

11-نظام مكافحة الجرائم المعلوماتية السعودي (2007م):

سَنَّت المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية، الذي أقرّه مجلس الوزراء الموقر برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز - حفظه الله - نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 3/8/ 1428 هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 3/7/ 1428هـ الذي يهدف إلى الحد من نشوء الجرائم المعلوماتية، وذلك بتحديد تلك الجرائم والعقوبات المقرَّرة لها.[13]

12-مشروع مكافحة الجرائم المعلوماتية المصري:

كان حرص المشرع المصري عظيمًا فى مواكبة النهضة التكنولوجية والمعلوماتية التى يعيشها العصر، فأصدر قانون خاص للاتصالات[14] (رقم10 /2003م) لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكترونى (رقم 2004/15م) لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية

---

(13) وجاء في المادة الثانية من هذا النظام: (يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1 – المساعدة على تحقيق الأمن المعلوماتي.

2 – حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3 – حماية المصلحة العامة، والأخلاق، والآداب العامة.

4 – حماية الاقتصاد الوطني).

(14) وعُرِّف الاتصالات في هذا القانون في (م1/ف3) بأنها: (أية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أياً كانت طبيعتها، وسواء كان الاتصال سلكياً أو لاسلكيًّا).

"الإنترنت"، فضلاً عن أنّ هناك جهودًا تبذل لإصدار قانون خاص بالمعاملات الإلكترونية لسلامة وتأمين المعاملات المختلفة من كافة جوانبها القانونية والجنائية، وهناك دراسات جادة لإعداد مشروع قانون لمكافحة الجريمة المعلوماتية.

13-القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة (2008م):
اعتمده مجلس وزراء العدل العرب بقرار رقم (771/د24 – 2008/11/27).

المبحث الثاني
أدلة إثبات الجرائم الإلكترونية
في الشريعة الإسلامية

- تعريف الإثبات:

الإثبات في اللغة مأخوذ من ثبت الشيء ثبوتًا، أي: دام واستقر، وثبت الأمر بنفسه، أي: عرفه حق المعرفة وأكّده بالبيّنات. فمادّة (ثبت) تفيد المعرفة والبيان والدوام والاستقرار، والمصدر: ثبات وثبوت وثبت، وأثبت حجّته: أقامها، **وعلى هذا فالإثبات في اللغة**: إقامة الحجّة على أمرٍ ما.[15]

ويؤخذ من كلام الفقهاء أنَّ الإثبات: إقامة الدليل الشرعي أمام القاضي في مجلس قضائه على حق أو واقعة من الوقائع.[16]

---

(15) انظر: مادة (ثبت): الصحاح للجوهري (245/1)، المصباح المنير (80/1)، لسان العرب (2/ 19)، تاج العروس (472/4)؛ د. عبدالرحمن بن عبد الله السند، حُجّية الوثيقة الإلكترونية، مجلة العدل، العدد (34).

(16) الموسوعة الفقهية الكويتية (232/1).

واستعمل الفقهاء الإثبات بمعناه اللغوي، وهو إقامة الحُجَّة، غير أنه يؤخذ من استعمالاتهم أنهم يطلقونه على معنيين خاص وعام:

فقد يطلقونه ويريدون به معناه العام، وهو إقامة الحُجَّة مطلقًا سواء أكان ذلك على حقٍّ أم على واقعة، وسواء أكان أمام القاضي أم أمام غيره، وسواء أكان عند التنازع أم قبله، حتى أطلقوه على توثيق الحق وتأكيده عند إنشاء الحقوق والديون، وعلى كتابة المحاضر والسجلات والدعاوى عند الكاتب العدل.

وقد يطلقون الإثبات ويريدون به معناه الخاص، وهو: إقامة الدليل أو الحُجَّة أمام القضاء، بالطرق التي حدّدتها الشريعة، على حق أو واقعة تترتب عليها آثار شرعية.

انظر: د. مصطفى الزحيلي، وسائل الإثبات (22/1)، حُجّية الوثيقة الإلكترونية، مجلة العدل، العدد (34).

والإثبات في القانون لا يخرج في تعريفه ومعناه عمّا ورد في الشريعة، وقد ذكر شُرّاح القوانين تعريفات كثيرة للإثبات، منها ما عرّفه الدكتور الصدة بقوله: (الإثبات هو إقامة الدليل أمامَ القضاء بالطريقة التي يحدّدها القانون على وجود حقٍّ مُنازَعٍ فيه). وعرّفه الدكتور السنهوي بقوله: (هو إقامة الدليل أمامَ القضاء بالطرق التي حدّدها القانون على وجود واقعةٍ قانونية تَرتّبت عليها آثارُها). والدليل له عدّة استعمالات منها أنّ كل وسيلة مستعملة للدفاع ولإظهار وجود فِعْل مُدَّعَى به ومُنْكَر من الخصم فهو دليل. والقانون لم يُبِح التمسُّك بأي دليل، وإنَّما حدّد طرق الإثبات، وعَيَّن مجال كل طريق من الطرق وحدودها التي يجوز فيها الإثبات.[17]

- حصر وسائل الإثبات:

طرق الإثبات في المواد الجنائية في الشريعة الإسلامية:

البيّنة، الإقرار، القرائن، الخبرة، معلومات القاضي، الكتابة، اليمين.

وهناك طريقان انفردت بهما الشريعة الإسلامية، وهما: القسامة واللعان.[18]

وذهب جمهور الفقهاء – رحمهم الله – إلى أنّ وسائل الإثبات محصورة فيما ورد به النص الشرعي صراحة، أو استنباطًا كالشهادة والإقرار واليمين، وقد اختلف أصحاب هذا القول في حصرها، فمنهم مَن حصرها في سبع، ومنهم من حصرها في ست، ومنهم من حصرها في ثلاث. واستدلّ أصحاب هذا القول بالأدلة التي فيها تحديد لطرق الإثبات، كقوله تعالى: ﴿**وَاسْتَشْهِدُوا شَهِيدَيْنِ مِنْ رِجَالِكُمْ فَإِنْ لَمْ يَكُونَا رَجُلَيْنِ فَرَجُلٌ وَامْرَأَتَانِ مِمَّنْ تَرْضَوْنَ مِنَ الشُّهَدَاءِ**﴾ [البقرة: 282]، وقوله تعالى: ﴿**يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوَّامِينَ بِالْقِسْطِ شُهَدَاءَ لِلَّهِ وَلَوْ عَلَى أَنْفُسِكُمْ**﴾ [النساء: 135] والشهادة على النفس إقرار، وحديث: «**اليَمِينُ عَلَى المُدَّعَى عَلَيْهِ**».[19] وفي زيادةٍ ليست في الصّحيحين وحسَّن إسنادَها الحافظ ابن حجر[20]: «**وَالْيَمِينَ عَلَى مَنْ أَنْكَرَ**»[21]. والمنكِر هو المدَّعَى عليه، وهو المطلوب كما أنَّ المدعي هو الطالب.[22]

---

(17) د. مصطفى الزحيلي، وسائل الإثبات (22/1).

(18) د. أحمد فتحي بهنسي، نظريه الإثبات في الفقه الجنائي الإسلامي (ص14).

وانظر: وسائل الإثبات (614/2 - 615).

(19) صحيح البخاري (4552)، صحيح مسلم (1711).

(20) فتح الباري (283/5).

وذهب جمعٌ مِن المحقّقين منهم شيخ الإسلام ابن تيمية وتلميذه ابن القيّم رحمهما الله[23]، إلى أنَّ وسائل الإثبات غير محصورة بعددٍ مُعَيَّن من وسائل الإثبات، بل تشمل كل ما يبيّن الحق ويُظهره. ومن أدلة هذا القول حديث ابن عباس: «**الْبَيِّنَةُ عَلَى الْمُدَّعِي**».[24]

وثبت عن النبي ρ أنه قال لِلْحَضْرَمِيِّ: «**أَلَكَ بَيِّنَةٌ؟**».[25] **والبينة في كلام الله ورسوله وكلام الصحابة اسم لكل ما يُبَيِّن الحق** من شهود أو دلالة؛ فهي أعم من البينة في اصطلاح الفقهاء، حيث خصوها بالشاهدين أو الشاهد واليمين، والشارع في جميع المواضع يقصد ظهور الحق بما يمكن ظهوره به من البينات التي هي أدلة عليه وشواهد له، ولا يُرد حقًّا قد ظهر بدليله أبدًا فيضيع حقوق الله وعباده ويعطّلها، ولا يقف ظهور الحق على أمر معين لا فائدة في تخصيصه به مع مساواة غيره في ظهور الحق أو رجحانه عليه ترجيحًا لا يمكن جحده ودفعه، كترجيح شاهد الحال على مجرد اليد في صورة من على رأسه عمامة وبيده عمامة، وآخر خلفه مكشوف الرأس يعدو أثره، ولا عادة له بكشف رأسه، فبيّنة الحال ودلالته هنا تفيد من ظهور صدق المدعي أضعاف ما يفيد مجرد اليد عند كل أحد؛ فالشّارع لا يهمل مثل هذه البيّنة والدلالة، ويضيع حقًّا يعلم كل أحد ظهوره وحجته، بل لما ظن هذا من ظنه ضيعوا طريق الحكم، فضاع كثير من الحقوق لتوقف ثبوتها عندهم على طريق معين، وصار الظالم الفاجر ممكنا من ظلمه وفجوره، فيفعل ما يريد، ويقول لا يقوم علي بذلك شاهدان اثنان، فضاعت حقوق كثيرة لله ولعباده، وحينئذ أخرج الله أمر الحكم العلمي عن أيديهم، وأدخل فيه من أمر الإمارة والسياسة ما يحفظ به الحق تارة ويضيع به أخرى، ويحصل به العدوان تارة

=

(21) أخرجها البيهقي في سننه الكبرى (426/10) من حديث ابن عباس، حسَّن إسنادها الحافظ ابن حجر في فتح الباري (283/5).

(22) كما جاء في حديث ابن عباس عند البيهقي في سننه الكبير (426/10).

(23) مجموع الفتاوى (392/35)، إعلام الموقعين (71/1)، الطرق الحكمية (25/1).

(24) أخرجه الشافعي (641 – سندي) من حديث ابن عباس. والترمذي في جامعه (1341)، وابن المقرىء في معجمه برقم: (616)، والدارقطني في سننه (4311) من طرق عن عمرو بن شعيب عن أبيه عن جدّه، به.

قال البغوي في شرح السنة (10/ 101): (هذا حديث صحيح). وقال الترمذي في جامعه (1342): (والعمل على هذا عند أهل العلم من أصحاب النبي ρ وغيرهم أنَّ البينة على المدعي، واليمين على المدعى عليه).

واعتبار أنَّ البينة على المدعي واليمين على المدعى **عليه**، من الأصول الشرعية. الجوهر النقي (120/8).

(25) صحيح مسلم (139).

والعدل أخرى، ولو عرف ما جاء به الرسول صلى الله عليه وسلم على وجهه لكان فيه تمام المصلحة المغنية عن التفريط والعدوان.[26]

وقال ابن القيّم رحمه الله: (لم تأت البينة قط في القرآن مرادا بها الشاهدان، وإنما أتت مرادا بها الحجة والدليل والبرهان ..، وكذلك قول النبي ρ: «**البينة على المدعي**»، المراد به: أنَّ عليه بيان ما يُصَحِّح دعواه ليُحْكَم له، والشّاهدان مِن البيّنة، ولا ريب أنّ غيرها مِن أنواع البيّنة قد يكون أقوى منها؛ لدلالة الحال على صدق المدعي؛ فإنها أقوى من دلالة إخبار الشاهد).[27]

وأمَّا أدلة الجمهور فهي لإثبات الوسائل المذكورة وأنها من وسائل الإثبات، لا أنها هي وحدها وسائل الإثبات، وبناءً على ذلك تكون وسائل الإثبات غير محصورة في عدد معيّن وطرق خاصّة، بل تكون غير محدّدة، وكل وسيلة تُظهر الحق، وتكشف عن الواقع يصح الاعتماد عليها في الحكم والقضاء بموجبها.[28]

ويظهر أنَّ الخلاف بين الجمهور وبين ابن تيمية وابن القيّم . رحم الله الجميع . في حصر طرق الإثبات في عدد معيّن وعدم حصره خلاف لفظي، فلو نظر الجمهور بما نظر إليه ابن تيمية وابن القيم لما قالوا بالحصر، ولو نظر ابن تيمية وابن القيّم إلى ما نظر إليه الجمهور لقالا بالحصر؛ لأنّ الجمهور لا يمنعون أيّة وسيلة يثبت بها الحق ويتأكّد منها القاضي وتلزمه الحكم بها، وتوجب على القاضي الحكم بها، فلا خلاف باعتبارها وسيلة شرعية في الإثبات، غير أنّ ابن القيّم يعتبرها وسيلة جديدة مستقلة، والجمهور يعتبرونها تحت ما ذكر من الوسائل والقواعد الكليّة لطرق الإثبات، وخصوصًا القرائن التي يدخل تحتها القيافة والعيافة والفراسة. والظاهر كذلك أنّ طرق الإثبات ليست تعبُّدية، ولكنها قابلة للتعليل، وأنَّ العلة فيها إظهار الحق وإثباته، وأنها خاضعة للاجتهاد، وبناء على ذلك تكون وسائل الإثبات غير محصورة في عدد معيّن وطرق خاصّة، بل تكون مطلقة وغير محدّدة، وكل وسيلة تُظهر الحق، وتكشف الواقع، يصح الاعتماد عليها في الحكم، والقضاء بموجبها، وإذا حُدِّدت وسائل الإثبات في قواعد عامّة، وصُنِّفَت في ضوابط كلية فإنّما يقصد منه التنظيم وسدّ

---

(26) إعلام الموقعين (71/1).

(27) الطرق الحكمية (25/1 – 26).

(28) انظر: وسائل الإثبات (615/2 – 616)، حُجِّية الوثيقة الإلكترونية، مجلة العدل، العدد (34).

الذرائع في الحدود التي خوّلها الشارع لوليّ الأمر، يتصرّف بما يراه مناسبًا للمصلحة العامة.[29] **وينبغي الحذر من تتبع هوى الخصوم، والحرية المطلقة للقاضي في تتبع الطرق الغريبة والغير معتبرة شرعًا أو نظرًا**؛ لِمَا يؤدّي ذلك من الفوضى، ويفتح مجال التلاعب والتزوير، وضياع أوقات القضاء، واستمرار المشاحنات وإتاحة الفرصة لقضاة الظلم والجور بادّعاء الإثبات وتأسيسه على الخيال والشكوك والأمارات الواهية، ولو تُرِكَ كل مُدَّعٍ يقيم دليله باجتهاده ولو كان مردودًا شرعًا أو نظرًا؛ لَعَمَّ الاضطراب وطال النزاع.

وتحديد طرق الإثبات تجعل أصحاب الحق على بينة ومعرفة واطلاع فيما يجب عليهم القيام به، وبما يلزمهم التمسك فيه أو إحضاره عند نشوء الحق ضمانًا من الجحود والإنكار، وأصول هذه الطرق:

1- **الشهادة**: وهي على مراتب وأنواع: شهادة أربعة رجال، شهادة رجلين، شهادة رجل وامرأتين. وهذه متفق عليها. واختلف في أنواع أخرى، وهي: شهادة الرجل واليمين، شهادة المرأتين واليمين، شهادة المرأة الواحدة، شهادة المرأتين فقط، شهادة الرجل الواحد.

2- **الإقرار**: ويشمل: الإقرار الصريح، والضمني، والإقرار باللفظ، وبالكتابة، وبالإشارة.

3- **اليمين**: وفيه أنواع: يمين المدعى عليه، واليمين المردودة، والمؤكّدة أو المتمّمة أو الاستظهار، والقسامة وأيمان اللعان.

4- **الكتابة**: وفيها فروع، منها: خط المورّث، خط الشاهد، كتاب القاضي إلى القاضي، سجلات القضاء، دواوين الدولة، الصكّ أو الحُجّة وغير ذلك.

5- **القرائن**: ويندرج تحتها أنواع كثيرة، منها: القيافة، والفراسة، واللوث في القسامة، ودلالة الحال أو ظاهر الحال، والصلاحية، والعرف، والعادة.

6- **المعاينة والخبرة**: وتشمل معاينة القاضي أو نائبه ، وخبرة المتخصّصين في كل علم أو فرع من فروع الحياة ويدخل فيها شهادة الطبيب، والبيطار، والمقوّم للمتلفات، والخارص، وشهادة القابلة، ورؤية الهلال، وغيرها مما يحتاج إلى مزيد علم ومعرفة وخبرة وتجربة في ناحية من نواحي الحياة والعلم بحيث لا يستطيع القاضي أو الإنسان العادي معرفتها بمجرد معلوماته العامة.

---

(29) انظر: وسائل الإثبات (2/615 - 616).

7- علم القاضي.[30]

المبحث الثالث
أدلة إثبات الجرائم الإلكترونية
في التشريعات العربية

تاريخ تشريعات الجرائم الإلكترونية وأدلة إثباتها :

تأسَّست **نظريّات الإثبات** على حقيقةٍ أساسيّة -كان للرومان قصب السبق في التعبير عنها - وهي أنَّ الحق المجرَّد عن الدليل لا وجود له، ويُعد عَدمًا عند حصول المنازعة.

وأمَّا **الإثبات الجنائي**، فهو: نشاط إجرائي مُوجَّه مباشرةً للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتّهام أوتأكيد أونفي آخر، يتوقَّف عليه إجراء قضائي.

وبمعنًى آخر، هو: إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين.

والهدف من الإثبات، هو: بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة؛ فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات.

ووسيلة الإثبات، هي: كل ما يستخدم في إثبات الحقيقة - فهي نشاط يُبذَل في سبيل اكتشاف حالة أو مسألة أو شخص أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة - أي: الأدلة - ونقلها إلى المجال الواقعي الملموس.[31]

وقد شهد مطلع التسعينات الهجرية (السبعينات الميلادية) الانطلاقة الحقيقيّة **لموجة** تشريعات الخصوصيّة، ومطلع السبعينات أيضًا وعلى امتداد العقدين بعدهما شهد انطلاقة **الموجة الثانية** المتمثّلة بقوانين جرائم الكمبيوتر، في حين شهدت التسعينات الهجرية (السبعينات الميلادية) البحث

---

(30) انظر: وسائل الإثبات (615/2 - 616).

وانظر: د. أحمد فتحي بهنسي، نظريه الإثبات في الفقه الجنائي الإسلامي (ص14 - وما بعدها)؛ عبدالله بن صالح بن رشيد الربيش، سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية، بحث تكميلي لنيل درجة الماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1423 / 1424 هـ؛ د. عارف خليل أبوعيد، جرائم الإنترنت - دراسة مقارنة، مصدر سابق.

(31) انظر: د. علي حسن الطوالبه - أستاذ القانون الجنائي المساعد، عميد كلية الحقوق، جامعة العلوم التطبيقية - البحرين، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي: دراسة مقارنة، مركز الإعلام الأمني، **2009**م.

الجدّي لحماية برامج الكمبيوتر ضمن نظام الملكيّة الفكريّة، وتحديدًا حق المؤلف، وانطلاق التدابير التشريعيّة الأولى في هذا الحقل؛ ليشهد أوائل هذا القرن الهجري فعليًّا انطلاقة **موجة ثالثة** من التشريعات المتصلة بالكمبيوتر هي موجة تشريعات حماية البرمجيات التي تمثّل المصنّف الأهم من بين عناصر تكنولوجيا المعلومات، التي ستفتح الباب أمام مفهوم المصنَّفات الرقميّة، واتّساع دائرة الحماية القانونيّة في نطاقها.

إذن، ثلاث موجات تشريعية، ولم يولد بعد قانون الكمبيوتر:

تشريعات الخصوصية (حماية الحق في البيانات الشخصية من مخاطر التكنولوجيا).

قوانين جرائم الكمبيوتر (الاعتداء على نُظُم المعلومات والمعلومات ببُعدها الاقتصادي).

وتشريعات حماية برامج الكمبيوتر (الملكية الفكرية) .

هذه الحقول الثلاثة في ساحة قانون الكمبيوتر، نشأ كل منها مستقلا عن الآخر، وفي إطار فرع قانوني مغاير للآخر:

حقوق الإنسان (بالنسبة للخصوصية).

والقانون الجزائي (بالنسبة لجرائم الكمبيوتر).

والملكية الفكرية: حق مؤلف، وبراءات اختراع (بالنسبة لحماية برامج الكمبيوتر وقواعد البيانات).

وأوّل الحقول التي برزت عقب الحقول الثلاثة المتقدِّمة: **قواعد الإجراءات الجنائية بشأن جرائم الكمبيوتر المتصلة بإجراءات الاستدلال والتحقيق والإثبات وإجراءات المحاكمة** المتفقة مع طبيعة الاعتداءات في الدعاوى التي تتعلق بجرائم الكمبيوتر، أو الاعتداء على الخصوصية، حتى في حقل قرصنة برمجيات الحاسوب المخزنة داخل النظم أو المحمّلة مع الأجهزة.

وبالرغم من أنّ الدول الأوروبية وأستراليا كذلك قد تنبّهت لهذا الموضوع مبكرًا مع مطلع التسعينات الهجرية (السبعينات الميلادية) ، إلا أنّ الموجة التشريعية المتصلة بهذه القواعد باتت حقيقة، وعلى نطاقٍ واسع في أوائل القرن الهجري الحالي ومنتصف الثمانينات (ابتداء من عام 1984 بريطانيا).

ومنذ نهاية السبعينات ومطلع الثمانينات كانت تثار في الإطار القانوني التساؤلات بشأن حُجِّيّة مستخرجات الكمبيوتر، ومشكلات الإثبات بواسطة ملفّات الكمبيوتر، والبيانات المخزَّنة فيه أيًّا كانت صورة هذه البيانات، وقد شهدت أوروبا تحديدًا نشاطًا محمومًا في هذا

الحقل، انطلق مع منتصف الثمانينات، وانصبّ على البحث في **تطوير قواعد الإثبات**، وأصول المحاكمات في المواد المدنيّة والتجاريّة لاستيعاب التوظيف المتنامي لأنظمة الكمبيوتر والاعتماديّة المتزايدة عليها، وما ينشأ عن ذلك من كثرة اللجوء لسجلات الكمبيوتر، وملفّات البيانات المخزَّنة للاحتجاج بها، ليس فقط تلك المخزَّنة في نُظُم المعلومات، بل سجلات وبيانات شبكات الاتصالات الخاصّة، كبيانات شبكة سويفت وغيرها الخاصّة بالعمل المصرفي، وبيانات أنظمة الشحن البحري الإلكترونيّة التي أخذت في الاتّساع والنَّماء، وبيانات سجلات الشبكات الاتصاليّة المختلفة؛ لكن هذه البدايات ما لبثت أنْ أخذت مَنْحًى مختلفاً تمامًا مع دخول الإنترنت في مطلع التسعينات الاستخدام التجاري الواسع؛ إذْ مع الاتجاه إلى التشبيك أو بناء شبكات المعلومات على نحوٍ واسعٍ، والتحوُّل مِن أنماط العمل الماديّ إلى العمل الإلكترونيّ، أصبح الأمر أكثر من مجرَّد حُجيّة مستخرجات نُظُم الكمبيوتر وشبكات الاتصال؛ بل أصبح مسائل التعاقدات ووسائل إثباتها في بيئة الشبكات والنُّظُم الإلكترونيَّة.[32]

***

طرق الإثبات الجنائي في قوانين الدول العربية :

لم تشهد **قوانين الإثبات العربية** تعديلات في حقل حجية مستخرجات الكمبيوتر والمواد الإلكترونية في النزاعات الحقوقية والتجارية، باستثناء التعديل الذي حصل على قانون البيّنات الأردني، ومشروع تعديل قانون أصول المحاكمات اللبناني.

والقاعدة في **الدعاوى الجزائية أو الجنائيَّة**: جواز الإثبات بكافَّة طرق الإثبات القانونيَّة؛ **فيحق للمدعي** أنْ يثبت دعواه بكافَّة هذه الطرق، **ويحق للقاضي** أنْ يُكَوِّنَ قناعته مِنْ أيِّ دليلٍ أو أمارةٍ أو إجراءٍ يُقَدَّم إليه، أو يطلع إليه بنفسه. ثم اقتضت الضرورة تقييد الوسائل بعددٍ مِنَ الطُّرق، **والقيد على هذه القاعدة**: أنَّ الدليل يتعيَّن أنْ يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهميَّة **اعتراف القانون** بالأدلة ذات الطبيعة الإلكترونيَّة. والمعلومات وإنْ كانت قيمتها تتجاوز شيئًا فشيئًا

(32) انظر: د. يونس عرب، حجية الإثبات بالمستخرجات الإلكترونية في القضايا المصرفية، مجلة البنوك – الأردن؛ ورشة عمل: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات: مسقط – سلطنة عمان، 2-4 ابريل 2006، ورقة عمل: قانون تكنولوجيا المعلومات.

الموجودات والطاقة؛ فانّها ليست ماديّات لتقبل بيّنة في الإثبات، ووسائط تخزينها – غير الورق كمخرجات – لا تحظى (من حيث محتواها) بقبولها دليلا ماديًّا، من هنا كان البحث القانوني في العديد من الدول يتجه إلى الاعتراف بالحجية القانونية لملفات الكمبيوتر ومستخرجاته والرسائل الالكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي، ولكن بطبيعتها الإلكترونيّة المحضة.

صعوبات الإثبات في الجرائم الإلكترونيّة :

المشكلة تكمن في القواعد المخَزَّنَة في صفحات الفضاء الإلكتروني في الوثيقة الإلكترونية؛ إذْ ما تحتويه مِنْ بياناتٍ، قد يكون الدليل على حصول تحريفٍ أو دخولٍ غير مصرَّح به أو تلاعب ... إلخ، فكيف يقبلها القضاء، وهي ليست دليلا ماديًّا يضاف الى الملف كالمبْرَز الخطِيّ أو (محضر) أقوال الشاهد أو تقرير الخبرة؟!.

ولتجاوز هذه المشكلة يَلجأ القضاء الى انتداب الخبراء[33] لإجراء عمليّات الكشف والتثبُّت من محتوى الوثائق الإلكترونية، ومن ثم تقديم التقرير الذي يُعد هو البيّنة والدليل، وليس الوثائق الالكترونية؛ لكنَّه مسلك تأباه بعض النُّظُم القانونيّة عِوَضًا عن معارضته لأسس وأغراض إجراء الخبرة، وطبيعتها كبيّنة تخضع للمناقشة والاعتراض، والرفض والقبول.[34]

وسائل الإثبات الإلكتروني:

أ ـ كيفية إنشاء وسائل الإثبات الإلكتروني:

باستعراض طرق الإثبات في القونين العربية نلمس أنها استوعبت كافة طرق الإثبات الممكنة في مجال الجرائم الإلكترونية.

- نص " **قانون الإثبات المصري الجديد** " على الأدلة التالية:

1- الكتابة[35] (المادة 10).

---

(33) وانتداب الخبراء طريق من طرق الإثبات المعترف بها قانونًا في التشريعات العربية، كما يأتي.

(34) انظر: د. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي – النادي العربي للمعلومات – دمشق.

(35) احتلّت الكتابة من بين الأدلّة القانونيّة منزلة مُتقدِّمة، وتحديدًا في المسائل المدنيّة والتصرُّفات العَقْدِيَّة، ففي النظام اللاتيني – ونموذَجيه القانونين الفرنسي والمصري – تُمَثِّل الكتابة أقوى الأدلة، في حين بقي للشهادة منزلة متقدِّمة في النظام الأنجلو أمريكي – ونموذَجيه القانونين الأمريكي والبريطاني –، مع اتجاهٍ في هذين النموذجين – بدرجات متفاوتة بينهما – إلى إعلاء شأن الكتابة =

2- شهادة الخصوم (م60)
3- القرائن (م99)
4- الإقرار أو استجواب الخصم (م105)
5- اليمين (م114)، 6- المعاينة (م131)، الخبرة (م135). وتعتبر هذه الأدلة منصوص عليها على سبيل الحصر لا يجوز الإثبات بغيرها.

- **قانون البيّنات السوري** نصت المادة الأولى منه على طرق الإثبات وهي:
1- الأدلة الكتابية
2- الشهادة
3- القرائن
4- الإقرار
5- اليمين
6- المعاينة والخبرة.

- **وقد خلت مواد قانون مكافحة الجرائم المعلوماتية الإماراتي رقم 2 لسنة (2006م)، ونظام مكافحة الجرائم المعلوماتية السعودي (1428هـ/2007م) من بيان تعيين طرق إثبات الجرائم المعلوماتية، وفي ذلك إشارة إلى قضيتين هامَّتين:**

الأولى: أنَّ السكوت عن بيان طرق الإثبات، فيه إشارة إلى إعمال وتطبيق القواعد العامة في الإثبات، وأنَّ الجرائم المعلوماتية مثلها مثل بقية الجرائم غير أنها تأخذ صورًا أكثر معاصرة وحداثة.

الثانية: الإشارة إلى صعوبة إثبات مثل هذه الجرائم؛ ولذلك جاء في نص المادة (24) من القانون الإماراتي ما نصه: (**مع عدم الإخلال بحقوق الغير حسن النية** يحكم في جميع الأحوال **بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم** المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، **كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي**

=

والتضييق من شأن الشهادة أو ما يُعبَّر عنه بالبيِّنة الشخصيَّة. انظر: د. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، مصدر سابق.

من هذه الجرائم إذا كانت الجريمة قد ارتُكِبَت بعلم مالكه، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة).

وكذلك جاء **في نص المادة (13) من نظام مكافحة الجرائم المعلوماتية السعودي**: (مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، **كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقّتًا متى كان مَصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتُكِبَت بعلم مالكه). وفي هاتين المادتين** إشارة إلى صعوبة إثبات مثل هذه الجرائم – وهذا واقع الأمر كما يأتي–؛ ولذلك عبّر المقنّن بقوله: (**وكانت الجريمة قد ارتُكِبَت بعلم مالكه) ففيه إشارة إلى جهالة الفاعل الأصلي وصعوبة تعيينه، ثم إذا تُوصِّل إليه بطرق الإثبات العامة المتقدِّم ذكرها؛ فإنَّه بعينه يقع تحت طائلة هذه المواد العقابيّة.**

وقد نصت المادة (14) من النظام السعودي على: تعاون هيئة الاتصالات وتقنية المعلومات على: (**تقديم الدعم والمساندة الفنيّة للجهات الأمنيّة المختصة خلال ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة**). وهذا النص المهم يعيدنا إلى اعتبار الخبرة كأحد طرق الإثبات المعتبرة شرعًا وقانونًا وقضاءً.[36]

ب ـ طرق اعتماد وسائل الإثبات الإلكتروني:

جاء في القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة (771/د24 – 2008/11/27)، في الفصل الثالث (**حجّية الكتابة والمحرّرات والتواقيع الإلكترونية**)، **ثم ذكر لهذه الحُجِّيَّة شروطًا، وهي:**

أ – ارتباط التوقيع الإلكتروني بالموقِّع وحده دون غيره.

ب – سيطرة الموقِّع وحده دون غيره على أداة إنشاء التوقيع الإلكتروني.

ج – إمكانية كشف أي تغيير في بيانات المحرَّر الإلكتروني أو التوقيع الإلكتروني بعد وضعه على أي محرَّر.

---

(36) وانظر: التفتيش في الجرائم المعلوماتية في النظام السعودي (مصدر سابق).

وجاء في المادة العاشرة من هذا الفصل:

(للمحرّر الإلكتروني صفة النسخة الأصلية، إذا توافرت فيه الشروط الآتية:

أ – أنْ تكون المعلومات الواردة به قابلة للحفظ والتخزين بحيث يمكن في أي وقت الرجوع إليها.

ب – أن يكون محفوظًا بالشكل الذي تمّ إنشاؤه أو إرساله أو تسلّمه أو بأي شكل يُسهّل دقّة المعلومات التي وردت به عند إنشائه أو تسلّمه.

ج – أن تدلّ المعلومات الواردة به على من أنشأه أو تسلَّمه وتاريخ ووقت إرساله وتسلّمه.

د – إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا).

وهكذا يكون **القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة** آنف الذِّكر قد اعتبر صراحةً **حُجيَّة الكتابة والمحرّرات والتواقيع الإلكترونية**، وعليه فإنَّه يؤخذ من ذلك اعتبار هذه المحرَّرات الإلكترونية أدلة إثبات يمكن الاحتجاج بها عند التنازع، يقول الدكتور يونس عرب: (الأدلة ذات الطبيعة الالكترونية يتعين مساواتها بالأدلة ذات الطبيعة المادية – الأدلة القائمة على الكتابة والورق – من حيث المقبوليَّة والحُجِيَّة .. وكلما كان التصرف المادي في البيئة الواقعية محل اعتبار يتعين الاعتراف بما يقابله من تصرف معنوي في البيئة الرقمية، فالتوقيع الالكتروني يقتضي مساواته بالتوقيع المادي . والتصديق الإلكتروني يتعين مساواته بالتصديق المادي، وهكذا، شريطة أن تحقق البيئة الرقمية من حيث المعايير والإجراءات المتصلة بالسلوكيات المعنوية أو سلوكيات البيئة الافتراضية ما يوفر الثقة التي تحلت بها السلوكيات المادية).[37]

- ثمَّ إنَّه ينبغي على القاضي أنْ يكونَ مُتفَهِّمًا لفحوى التقدُّم التِّقَنِيّ، وما ينتج عنه من وسائل إجرامية يغلب عليها هذا الطابع التقني الحديث.

وعلى هذا الأساس، ينبغي أنْ يَقْبَلَ بالأدلَّة المستمدَّة من الكمبيوتر لإثبات وقائع الدعوى التي تتناول جرائم المعلوماتيَّة، ويساعده في هذا الأمر طرق وقواعد ومبادئ الإثبات العامَّة، والقناعة الشخصيَّة للقاضي في المجال الجنائي.

ومن ناحيةٍ أخرى؛ فإنَّه ينبغي على القاضي أنْ يتحلَّى بالمقدرة على التكييف القانوني للأفعال الجرميّة المستحدثة، مع التشريعات التجريميّة القائمة.[38]

***

(37) د. يونس عرب، التدابير التشريعية، مصدر سابق.

(38) انظر: القاضي: وليد عكوم، التحقيق في جرائم الحاسوب، الدليل الإليكتروني للقانون العربي، (ص8).
وانظر: د. علي حسن الطوالبه، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، مصدر سابق.

المبحث الرابع
صعوبات إثبات الجريمة الإلكترونية

بخلاف ما يتصوَّره كثير من الباحثين والمختصّين في مجال مكافحة الجريمة المعلوماتية، فإنَّ ظاهرة انتشار التشريعات والقوانين للحد من هذه الآفة أخذت في الازدياد في كثير من دول العالم. وأغلب هذه القوانين لم تأخذ في الاعتبار عند إنشائها أنَّ الجريمة المعلوماتيَّة تنشأ في بلد ليحدث أثرها في بلد آخر.

ومن الأمثلة الواقعيَّة على ما تقدَّم ما حَصَلَ في دولة الإمارات العربية المتحدة، حيث قام مُشَغِّل حاسوب بتهديد المؤسَّسة التي يعمل لديها بتنفيذ مجموعة من مطالبه، وذلك بعد أنْ حذف كافّة البيانات الموجودة على الجهاز الرئيسي للمؤسّسة، وقد رفضت المؤسسة الاستجابة لمطالبه، فأقدم على الانتحار، ووجدت المؤسسة صعوبة في استرجاع البيانات التي كانت قد حُذفت.

وتتعقد المشكلة عندما يتعلَّق الأمر بمعلومات أو بيانات تم **تخزينها في الخارج** بواسطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثًا عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية؛ حيث إن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة، ولما كانت أدلة الإثبات المتحصِّلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنيّة، ودراية فائقة في هذا المجال؛ فإنَّ نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدِّي إلى ضياع الدليل بل تدميره أحيانًا، ويضاف إلى ذلك أنَّ كل المعطيات ليس لها تجسيد دائم على أية دعامة، بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة ولا على أية دعامة مادية منقولة أيًا كانت، فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية إلا أنّه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية، وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن الجرائم المعلوماتية إلى السلطات المختصة، بالإضافة لما تقدم من صعوبات ومشكلات.[39]

---

(39) د. علي حسن الطوالبه، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي: مصدر سابق.

وتقدَّم أنَّ الجرائم الإلكترونية هي (**الجرائم النظيفة**)؛ **وذلك** لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأيَّة عنف أو دماء، وإنما مجرد أرقام وبيانات **يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي**.(40)

ومن هنا نقف على حقيقة الصعوبات التي تواجه كافة أطراف المنظومة الأمنية والقضائيّة في هذا الصدد، التي تتجلَّى عندما تكون الجريمة واقعة على برامج الكمبيوتر وبياناته أو بواسطتها، وذلك بالنظر إلى قلّة الآثار الماديّة التي قد تنتج عن هذا النوع من الجرائم، وكثرة عدد الأشخاص الذين قد يتردَّدُون على مسرح الجريمة خلال المدَّة الفاصلة بين وقوع الجريمة والكشف عنها.

ومما تقدم نخلص إلى أبرز الصعوبات التي تعترض إثبات الجريمة الإلكترونية:

1. **البعد الدولي**: يجري النفاذ إلى أنظمه الحاسوب في أحد البلدان ويتم التلاعب بالبيانات في بلد آخر وتسجّل النتائج في بلد ثالث، ناهيك عن أنَّه يمكن تخزين أدلة الجريمة الإلكترونية في جهاز حاسوب موجود في بلد غير الذي ارتكب فيه المجرم فعله، بالتالي يستطيع المجرم الإلكتروني إخفاء هويته، ونقل المواد من خلال قنوات موجودة في بُلدان مختلفة، في قارات مختلفة قبل الوصول إلى المرسَل إليهم، نتيجة القدرة على التنقل إلكترونياً من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارَّات مختلفة، بحيث تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك، مما يشكل تحدياً أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها(41).

(40) محمد علي العريان، الجرائم المعلوماتية، مصدر سابق.

وانظر: عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت «دراسة مسحيَّة على ضباط الشرطة في دولة البحرين»، أكاديمية نايف العربية للعلوم الأمنيّة، 1420هـ 1999م؛ رامي علي وشاح، الصعوبات الماديّة التي تعترض الإثبات بالمحرّرات الإلكترونية، الأكاديمية للدراسات الإجتماعية والإنسانيَّة، 3-2010 (ص44 – 52)؛ بدور عبدالله الملحم، تحديات نظام مكافحة الجرائم الإلكترونية السعودي، مركز التميُّز لأمن المعلومات؛ د. ناول عبدالهادي، تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت، مجلة العدل، العدد 31 رجب 1427.

(41)الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية، ضمن أعمال الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، 20-19 نيسان/يونيو 2007،المملكة المغربية،(ص 119).

2. **مهارة التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجردة.**

3. **تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال.**

4. **سهولة محو الأدلة** في زمن قصير.

لأجل هذه الصعوبة فإنَّ إعداد رجال الضبط الجنائي وقضاة الحكم، للبحث عن أدلة الإثبات في ميدان الجرائم المعلوماتية، يكتسب أهمية بالغة؛ إذ لا بد لهم من الدراية الكافية لطبيعة هذا النوع من الجرائم، الذي يتسم الكشف عنه وإثباته بصعوبات بالغة، وفي عالم «المعلوماتية وشبكات الكمبيوتر» القائم على تقنية الاتصالات والتوصيلات والوسائط الإلكترونية، لا تستطيع سلطة البحث والتحري والتحقيق تطبيق الإجراءات التقليدية على غالبية جرائم تقنية المعلومات. من أجل ذلك لا بد من تدريب وتكوين رجال الضبط الجنائي و التحقيق والقضاة المختصين بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة وفيما يتعلق بالكشف عنها، والقرائن والدلائل والأدلة المستحدثة في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصها فنيا، مع ضرورة تدريب القضاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها. وتكمن الصعوبة الأساسية التي تعترض سلطات البحث والتحري في ميدان الجرائم المعلوماتية، أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثارًا تدل على ارتكابهم لهذه الجرائم؛ إذْ تكون المعلومات محفوظة تحت رقم أو رمز سري أو مشفرة كليًّا؛ إذْ يصعب الولوج إليها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء الجناة؛ لذا لا بد من خلق وحدات خاصة تكون مهمتها الأساسية هي مراقبة وتتبع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة القبلية قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها.[42]

لذا لابد للحفاظ على مسرح الجريمة مايلي:

---

(42) السيد عبدالرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، 20 – 19 نيسان/ يونيو، 2007، المملكة المغربية، (ص71 – 72).

1-تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقّة تامّة، وأخذ صورة لأجزائه الخلفيّة وسائر ملحقاته.

2-ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة.

3-إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.

4-عدم التسرُّع في نقل أي مادّة معلوماتيّة من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة.[43]

***

التوصيات والمقترحات:

1- تفعيل دور المكافحة الوقائية التي تسبق وقوع الجريمة الإلكترونية، وذلك من خلال تفعيل دَور المؤسسات التوعويَّة (المسجد، الأسرة، دُور التعليم، أجهزة الإعلام)، وذلك بالتوعية بخطورة الجرائم الإلكترونية على الأسرة والمجتمع، والسعي في تقوية الوازع الديني.[44]

(43) انظر: وليد عكوم، التحقيق في جرائم الحاسوب، مصدر سابق، (ص6).

(44) وانظر: د. فايز بن عبدالله الشهري، دراسة الظاهرة الإجرامية على شبكة الإنترنت، مصدر سابق، (ص148 – وما بعدها).

2- إنشـاء مـدارس ومعاهـد وأقسـام في الجامعـات وكراسـي بحثيـة خاصّـة تعـنى بـالأمن المعلوماتي[1] والتدريب فيه، ومواكبة كل ما هو حديث في هذا المجال.

3- سَنّ القوانين والأنظمة الخاصَّة التي تسدُّ كافَّة ثغرات الجريمة الإلكترونية، مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها، والنصِّ على طرق ثبوتها.

4- التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعيّة، والقضائيّة، والضبطية، والفنية، وذلك من أجل سد منافذ الجريمة الإلكترونية قدر المستطاع، والعمل على ضبطها وإثباتها بالطرق القانونية والفنيّة.

5- إنشـاء قـانون دولي مُوَحَّـد، ومحـاكم خاصَّـة دوليَّـة محايـدة تتـولَّى التحقيـق في الجـرائم الإلكترونية، ويكون لها سلطة الأمر بضبط وإحضار المجرم الإلكتروني للتحقيق معه أيًّا كـان موقـع هـذا المجـرم وبلـده، وهـذا الاقـتراح أو التوصـية تتناسـب مـع مقـام الجريمـة الإلكترونيـة الـتي تتمثَّـل الكـرة الأرضـيَّة أمامهـا قريـة صـغيرة واحـدةً قريبـة المـدى متقاربـة الأطراف.

6- عقد الاتفاقيات بين الدول بخصوص الجرائم الإلكترونية وقايةً وعلاجاً وتبادلاً للمعلومات والأدلة.

7- التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضدّ دول أو جهات أخرى خارج هذه الأراضي.

8- تفعيل اتفاقيات تسليم المجرمين الإلكترونيين.

---

(1) تعتبر جامعة الأمير نايف ــ رحمه الله ــالعربية للعلوم الأمنية من الجامعات الرائدة في هذا المجال.